UNIVERSITY OF ILLINOIS
COLLEGE OF MEDICINE AT PEORIA

Policies, Procedures, Forms, Guides

Remote Access Policy and Approval Form

Responsible Office	**CIS**	**Effective Date**	**03/26/2009**
Responsible Official	**Christopher Lamer**	**Last Revision**	**03/26/2009**

Policy Sections

1.1 Purpose

The University's Combined Covered Entity including the College of Medicine is committed to securing and protecting Protected Health Information in accordance with information systems security best practices and the standards established by the Department of Health and Human Services under the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

The purpose of this policy is to define standards for connecting to University of Illinois College of Medicine at Peoria (UICOMP) network resources from any host. These standards are designed to minimize the potential exposure to UICOMP from damages which may result from unauthorized use of UICOMP resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical UICOMP internal systems, etc.

1.2 Scope

This policy applies to all UICOMP employees, contractors, vendors and agents with a UICOMP-owned or personally-owned computer or workstation used to connect to the UICOMP network. This policy applies to remote access connections used to do work on behalf of UICOMP, including reading or sending email and viewing intranet web resources.

Remote access implementations that are covered by this policy include, but are not limited to, dial-in modems, frame relay, ISDN, DSL, VPN, SSH, and cable modems, etc.

1.3 General

1. It is the responsibility of UICOMP employees, contractors, vendors and agents with remote access privileges to UICOMP's corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to UICOMP.

2. Access to the UICOMP network should not be shared with anyone. The UICOMP employee is responsible for this connection and that they do not perform illegal activities, and does not use the access for outside business interests. The UICOMP employee bears responsibility for the consequences should the access be misused.

3. Please review the following policies for details of protecting information when accessing the college network via remote access methods, and acceptable use of UICOMP's network:

*a. Acceptable Use Policy (*http://www.uic.edu/depts/accc/policies/uicpol.html *)*

b. Information Security Policy – University of Illinois
*(*http://www.obfs.uillinois.edu/manual/central_p/sec19-5.html *)*

1.4 Requirements

1. Secure remote access must be strictly controlled. Control will be enforced via your netID and Microsoft Active Directory password. For information on creating a strong password see the Password Policy (http://www.uic.edu/depts/accc/accts/altpswd.html#strongdef).

2. At no time should any UICOMP employee provide their login or email password to anyone, not even family members.

3. Personal equipment that is used to connect to UICOMP's networks must meet certain requirements. Non-standard hardware configurations must be approved by CIS.

4. All hosts that are connected to UICOMP internal networks via remote access technologies must use the most up-to-date anti-virus software (http://webstore.illinois.edu/). This includes personal computers.

5. The UICOMP employee is not to store high risk or confidential data on their local computer. Any data that might be downloaded to the local computer must be deleted, moved to a secure location, or encrypted as soon as practical.

1.5 Violations

Any individual, found to have violated this policy, may be subject to disciplinary action up to and including termination of employment as outlined in the ACCC Acceptable Use Policy at http://www.uic.edu/depts/accc/policies/uicpol.html and the ACCC Schedule of Penalties for Computing Privilege Abuse at http://www.uic.edu/depts/accc/policies/abuse.html.

Violations of policies such as the ACCC Acceptable Use Policy, Network Policy at: http://www.uic.edu/depts/accc/policies/netpol.html, Netid Policy at: http://www.uic.edu/depts/accc/policies/netid_changes.html and the Information Security Policy – U of I at http://www.obfs.uillinois.edu/manual/central_p/sec19-5.html and the U of I Web privacy Policy at: http://www.vpaa.uillinois.edu/policies/web_privacy.asp, should be reported to the HIPAA Security Officer, business unit management and College of Medicine administrative personnel. Based on the severity of the violation, notice of the violation should be forwarded to the University HIPAA Security Officer.

1.6 Employee Information

Full Name (please print):

_____

University ID Number: _____

netID: _____

Department: _____

Phone Number: _____

Computer Operating System (Microsoft XP, Vista, MAC OSX Version):

_____

Employee Signature*: _____

Date: _____

**By signing you agree to the above Remote Access Policies and fully understand and agree to comply with these policies and any policies outlined in this document.*

1.7 Department Approval

Department Authorized Signature**: Date:

_____ _____

Signature Name Printed:

_____

CIS Authorized Signature: Date:

_____ _____

CIS Name Printed:

_____

*** By signing this you agree that the above employee should be give rights to remotely access UICOMP resources.*

Revision History

First Issued 03/26/2009